WHAT IS CLAIMED AS THE INVENTION IS:

1. A system of securely controlling a wireless mobile communication device, comprising:

a plurality of domains residing on a wireless mobile communication device, each domain including an asset of the wireless mobile communication device; and

a domain controller configured to receive a request to perform an operation affecting at least one of the assets, to determine whether the request originated with an entity that has a trust relationship with the domain that includes the at least one affected asset, and to permit completion of the operation where the request originated with an entity that has a trust relationship with the domain that includes the at least one affected asset.

2. The system of claim 1, further comprising a key store for storing cryptographic keys associated with the domain that includes the at least one affected asset, wherein the domain controller is configured to determine whether the request originated with an entity that has a trust relationship with the domain using the cryptographic keys.

3. The system of claim 1, wherein the domain controller is configured to determine whether the request originated with the entity that has a trust relationship with the domain that includes the at least one affected asset by determining whether the domain that includes the at least one affected asset also includes the entity.

4. The system of claim 1, wherein the at least one domain further includes a software application.

5. The system of claim 4, wherein at least one of the domains comprises a plurality of domains, and wherein the wireless mobile communication device further comprises a super user software application that has a trust relationship with more than one of the plurality of domains.

6. The system of claim 5, wherein each of the more than one of the plurality of

AMENDED SHEET

domains includes the super user software application.

7. The system of claim 1, wherein the domain controller is further configured to receive information, and to place the information into a domain.

8. The system of claim 1, wherein the at least one asset is selected from the group consisting of: communication pipes, persistent data, properties, and software applications.

9. The system of claim 1, further comprising a data store for storing properties, wherein the domain controller is further configured to determine whether the operation is permitted by properties in the data store, and to permit completion of the operation where the operation is permitted by the properties in the data store.

10. The system of claim 9, wherein each property is global, domain-specific, or specific to a particular software application on the wireless mobile communication device.

11. A method for secure control of a wireless mobile communication device, comprising:

segregating assets of the wireless mobile communication device into a plurality of domains, each domain including at least one asset of the wireless mobile communication device;

receiving a request to perform an operation affecting at least one of the assets;

determining whether the operation is permitted by the domain that includes the affected asset; and

allowing the operation to be completed where the operation is permitted by the domain that includes the affected asset.

12. The method of claim 11, wherein the step of determining comprises the step of determining whether the request originated with an entity that has a trust relationship with the domain that includes the at least one affected asset.

13. The method of claim 12, wherein the step of determining whether the request originated with an entity that has a trust relationship with the domain that includes the at least one affected asset comprises the step of determining whether the domain that includes the at least one affected asset also includes the entity.

14. The method of claim 12, wherein the request originates from a software application, and wherein the step of determining whether the request originated with an entity that has a trust relationship with the domain that includes the at least one affected asset comprises the step of verifying a digital signature of the software application using a cryptographic key associated with the domain.

15. The method of claim 11, further comprising the steps of:
receiving information; and
associating the information with at least one of the plurality of domains.

16. The method of claim 15, wherein the step of associating comprises the step of determining with which domains the information is to be associated in accordance with domain policies.

17. The method of claim 16, wherein the domain policies specify that information is to be associated with domains based on one or more of: a source of the information, an indicator of a domain in the information, a communication pipe over which the information is received, a digital signature of the information, an access list describing allowed domain information, and an input from a user of the wireless mobile communication device.

18. The method of claim 11, further comprising the step of:
determining whether the operation is permitted by properties stored at the wireless mobile communication device,
wherein the step of allowing comprises the step of allowing the operation to be completed where the operation is permitted by both the domain and the properties.

19. The method of claim 18, wherein the step of determining whether the operation is permitted by properties stored at the wireless mobile communication device comprises the step of checking global properties for the wireless mobile communication device and domain properties for the domain that includes the at least one affected asset.

20. The method of claim 19, wherein the request originates from a software application, and wherein the step of determining whether the operation is permitted by properties stored at the wireless mobile communication device further comprises the step of checking application properties for the software application.